Password Policy and Procedures

1.0 Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in a compromise of <Agency Name>'s entire network. As such, all <Agency Name> employees (including contractors and vendors with access to <Agency Name> systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their password.

2.0 Purpose

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.

3.0 Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any <Agency Name> facility, has access to the <Agency Name> network and/or NCIC network, or stores any non-public <Agency Name> information.

4.0 Policy

4.1 General

- All systems-level passwords (e.g., root, enable, network administrator, application administration accounts, etc.) must be changed at least every 90 days.
- All production system-level passwords must be part of the Information Security administrated global password management database.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 90 days.
- User accounts with access to NCIC privileges must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.

- Where simple network management protocol (SMTP) is used, the community strings must be defined as something other than the standard defaults of "public," "private," and "system" and must be different from passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).

- All user-level, system-level, and NCIC access level passwords must conform to the guidelines described below.

4.2 Guidelines

General Password Construction

Passwords are used for various purposes at <Agency Name>. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e., Dynamic passwords which are used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters.

- The password is a word found in a dictionary (English or foreign)

- The password is a common usage word such as:

  - Name of family, pets, friends, co-workers, fantasy characters, etc.
  - Computer terms and names, commands, sites companies, hardware, software.
  - The words "<Agency Name>," "WVSP," "HPD," "CKSFP" or any derivation.
  - Birthdays and other personal information such as addresses and phone numbers.
  - Word or number patterns like aaabbb, 111222, zyxwvts, 4654321, etc.
  - Any of the above spelled backward like nhoj, yrrehckcalb, yffulf, etc.
  - Any of the above preceded or followed by a digit (e.g., secret1, 1secret).

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)

- Have digits and punctuation characters as well as letters, e.g., 0-9, !@#$%^&*()_+{}[]:";<>?,.?
- Are at least eight alphanumeric characters long.
- Are not a word within any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation. **NOTE: Do not use either of these examples as passwords**

4.3 Password Deletion

All passwords that are no longer needed must be deleted or disabled immediately. This includes, but is not limited to, the following:

- When a user retires, quits, is reassigned, released, dismissed, etc.
- Default passwords shall be changed immediately on all equipment.
- Contractor accounts, when no longer needed to perform their duties.

When a password is no longer needed, the following procedures should be followed:

- Employee should notify his or her immediate supervisor.
- Contractor should inform his or her point-of-contact (POC).
- Supervisor or POC should fill out a password deletion form and send it to <Agency's POC>.
- <Agency's POC> will then delete the user's password and delete or suspend the user's account.
- A second individual from that department will check to ensure that the password has been deleted and user account was deleted or suspended.
- The password deletion form will be filed in a secure filing system.

4.4 Password Protection Standards

Do not use your user id as your password. Do not use the same password for <Agency Name> accounts as for NCIC accounts. For example, select one password for your Windows account login and a different one for your NCIC account login. Do not share <Agency Name>

passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential <AgencyName> information.

Here is a list of "do not's"

- Don't reveal a password over the phone to anyone
- Don't reveal a password in an mail message
- Don't reveal a password to the boss
- Don' talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to a co-worker while on vacation
- Don't use the "Remember Password" feature of applications
- Don't write passwords down and store them anywhere in your office.
- Don't store passwords in a file on ANY computer system without encryption.

If someone demands a password, refer them to this document or have them call <list name of Information Security Officer (ISO) or Agency POC.

If an account or password is suspected to have been compromised, report the incident to <Name of ISO or POC> and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by the FBI or <Agency Security Department or POC>. If a password is guessed or cracked during one of these scans, the user will be required to change it.

C. Application Development Standards

Application developers must ensure their programs contain the following security precautions:

- Should support authentication of individual users, not groups.

- Should not store passwords in clear text or in any easily reversible form.

- Should provide some sort of role management, such that one user can take over the function of another without having to know the other's password.

- Should support Terminal Access Controller Access Control System+ (TACACS+), Remote Authentication Dial-In User Service (RADIUS), and/or X.509 with Lightweight Directory Access Protocol (LDAP) security retrieval, wherever possible.

D. Remote Access Users

Access to the <Agency Name> networks via remote access is to be controlled by using either a Virtual Private Network (in which a password and user id are required) or a form of advanced authentication (i.e., Biometrics, Tokens, Public Key Infrastructure (PKI), Certificates, etc.).

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.